

## ITL FOCUSES ON PUBLIC SAFETY COMMUNICATIONS

In collaboration with NIST's Office of Law Enforcement Standards (OLES) and the National Telecommunications and Information Administration, ITL demonstrated the Department of Commerce ISSI Evaluation and Test System (DIETS) at a recent Telecommunication Industry Association (TIA) Mobile and Personal Radio Standards meeting in Dallas, Texas. The TIA/TR8 standards committee is responsible for the so-called *Project-25* suite of interoperability standards for digital two-way wireless communications among public safety personnel. The DIETS project addresses the urgent need for expedited development and testing of the Inter-RF-Sub System Interface (ISSI), which is the key interoperability standard to enable communication among distinct public safety communication networks.

Not only is DIETS an interoperability and conformance test system for the key interoperability protocol of the Project-25 suite, but it embodies open source reference implementations of the ISSI protocols. The availability of such implementations will help jump start the industry in delivering commercial implementations. The novel DIETS architecture allows both local and remote testing of emerging commercial ISSI implementations for conformance, performance, and interoperability. For further information and access to this publicly available tool, see <http://www.x.antd.nist.gov/proj25/>.

## Software Tool for Parallel Solution of Partial Differential Equations

ITL recently released Version 1.0 of PHAML, a computer program for the solution of elliptic partial differential equations. PHAML stands for Parallel

Hierarchical Adaptive Multi-Level, which characterizes the methods upon which the software is based. The package is the culmination of a decade of research on advanced solution methods, including high-order finite elements, adaptive mesh refinement, multigrid solution techniques, dynamic load balancing, and parallel computing.

PHAML addresses problems that are found in a wide variety of models of physical phenomena, from the diffusion of heat in metal to the energy levels of atoms, and hence their efficient solution is of high interest. Earlier beta releases of the program have been used for a variety of purposes, including solution of scientific and engineering applications, a platform for the investigation of new numerical methods and approaches to programming parallel computers, and a classroom tool for studying numerical methods or parallel computing. PHAML can be freely downloaded and redistributed at <http://math.nist.gov/phaml/>.

## New Health Information Technology Website

ITL has launched the Health Information Technology (HIT) Implementation Testing and Support website at <http://hit-testing.nist.gov>. The site was developed by NIST in partnership with the American National Standards Institute (ANSI) Healthcare Information Technology Standards Panel (HITSP), the Certification Commission for Health Information Technology (CCHIT), and the Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC).

The website is a starting point for providing HIT implementers with access to the tools and resources

needed to support and test the implementation of standards-based health systems. The site currently provides information about ONC's Nationwide Health Information Network, CCHIT, HITSP, HISTP's Interoperability Specifications, the standards referenced by these specifications, and test resources. Also provided are pointers to the specifications and publicly available test tools; however, NIST is not performing operational testing or certification services.

## FEDERAL INFORMATION PROCESSING STANDARD (FIPS) ACTIVITIES

### ITL Seeks Public Comment on Draft FIPS 140-3, *Security Requirements for Cryptographic Modules*

In a Federal Register notice dated July 13, 2007, ITL announced the release of draft FIPS 140-3 for public review and comment. FIPS 140-3 will replace the current FIPS 140-2, *Security Requirements for Cryptographic Modules*. In addition to updates and clarifications, draft FIPS 140-3 addresses the issue of protecting smart cards from power analysis attacks. For a copy of the draft FIPS, see <http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf>. Electronic comments may be submitted to FIPS [140-3@nist.gov](mailto:140-3@nist.gov) by October 11, 2007.

### Two Additional Draft FIPS Released for Public Review

A Federal Register notice on June 12, 2007, announced the release of two draft FIPS for public review and comment:

Draft FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, is the proposed revision of FIPS 198. The draft FIPS 198-1 is the proposed revision of FIPS 198. The draft specifies a keyed-hash message



If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:

ITL Newsletter  
National Institute of Standards and Technology  
100 Bureau Drive  
Stop 8900  
Gaithersburg, MD 20899-8900

You will be placed on this mailing list only.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is <http://www.itl.nist.gov>.

ITL Editor: Elizabeth B. Lennon  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 8900  
Gaithersburg, MD 20899-8900  
Phone: (301) 975-2832  
Fax: (301) 975-2378  
E-mail: [elizabeth.lennon@nist.gov](mailto:elizabeth.lennon@nist.gov)

authentication code, a mechanism for message authentication using cryptographic hash functions and shared secret keys.

Draft FIPS 180-3, *Secure Hash Standard (SHS)*, is the proposed revision of FIPS 180-2. The draft specifies five secure hash algorithms (SHAs) called SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512, which are used to condense input messages to fixed-length messages, called message digests. These algorithms produce 160, 256, 384, and 512-bit message digests, respectively.

Comments on these two FIPS must be received by September 10, 2007. To review the draft FIPS and submit comments, see <http://csrc.nist.gov/publications/drafts.html>.

## NEW ITL PUBLICATIONS

### *Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information*

By Robert M. McCabe and Elaine M. Newton

NIST Special Publication 500-271  
May 2007

<http://fingerprint.nist.gov/standard/index.html>

This standard defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, scar, mark, & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, other recommended best practice image capture settings, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images. This information is intended for interchange among criminal justice administrations or other organizations that rely on the automated fingerprint information system (AFIS) and the palmprint identification system or use facial, SMT, iris, or other biometric data for identification purposes.

### *Source Code Security Analysis Tool Functional Specification Version 1.0*

By Paul E. Black, Michael Kass, and Michael Koo

NIST Special Publication 500-268  
May 2007

[http://samate.nist.gov/docs/source\\_code\\_security\\_analysis\\_spec\\_SP500-268.pdf](http://samate.nist.gov/docs/source_code_security_analysis_spec_SP500-268.pdf)

This document specifies the behavior of one class of software assurance tool, the source code security analyzer. Because many software security weaknesses today are introduced at the implementation phase, using a source code security analyzer should help assure that software doesn't have

many security vulnerabilities. This specification defines a baseline capability to help software professionals understand how a tool will meet their software security assurance needs.

### *A Scheme for PIV Visual Card Topography*

By William MacGregor, Teresa Schwarzhoff, and Ketan Mehta  
NIST Special Publication 800-104  
June 2007

[http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29\\_2007-final.pdf](http://csrc.nist.gov/publications/nistpubs/800-104/SP800-104-June29_2007-final.pdf)

This document provides additional recommendations on the Personal Identity Verification (PIV) Card color-coding for designating employee affiliation. The recommendations in this document complement FIPS 201 in order to increase the reliability of PIV card visual verification.

### *Guidelines on Cell Phone Forensics*

By Wayne Jansen and Richard Ayers  
NIST Special Publication 800-101  
May 2007

<http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>

This guide provides an in-depth look into cell phones and explains associated technologies and their affect on the procedures followed by forensic specialists. It also discusses procedures for the preservation, acquisition, examination, analysis, and reporting of digital information present on cell phones, as well as available forensic software tools that support those activities.

### *Guidelines for Securing Radio Frequency Identification (RFID) Systems*

By Tom Karygiannis, Bernard Eydt, Gregory Barber, Lynn Bunn, and Ted Phillips  
NIST Special Publication 800-98  
May 2007

[http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98\\_RFID-2007.pdf](http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf)

This publication seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world advice on how to initiate, design, implement and operate RFID systems in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls.

#### ***Border Gateway Protocol Security***

By Rick Kuhn, K. Sriram, and Doug Montgomery

NIST Special Publication 800-54

July 2007

<http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>

This document introduces the Border Gateway Protocol (BGP), explains its importance to the Internet, and provides a set of best practices that can help in protecting BGP. Best practices described here are intended to be implementable on nearly all currently available BGP routers. While a number of enhanced protocols for BGP have been proposed, these generally require substantial changes to the protocol and may not interoperate with current BGP implementations.

#### ***Quality Summarization, Recommendations on Biometric Quality Summarization across the Application Domain***

By Elham Tabassi and Patrick Grother

NISTIR 7422

May 2007

<http://www.itl.nist.gov/iad/894.03/quality/reports/enterprise.pdf>

This document is a set of recommendations to users of biometric quality assessment algorithms. In

particular it is concerned with aggregation of quality values across an enterprise appropriate to quantify estimated relative error rates.

#### ***Common Industry Specification for Usability—Requirements***

By Mary Theofanos

NISTIR 7432

June 2007

<http://zing.ncsl.nist.gov/iusr/documents/CISU-R-IR7432.pdf>

The Common Industry Specification for Usability - Requirements (CISU-R) helps usability professionals, product managers, and others working in product design and development to create usability requirements. It sets standards for specifying usability requirements, which include three types of information: the context of use - the intended users, their goals and tasks, associated equipment, and the physical and social environment in which the product can be used; performance and satisfaction criteria - measures of usability for the product; and the test method and context of testing - the method to be used to test whether the usability requirements have been met and the context in which the measurements will be made.

#### ***"ITL" Available Via E-Mail***

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to [litproc@nist.gov](mailto:litproc@nist.gov) with the message **subscribe itl-newsletter**, and your name, e.g., John Doe. For instructions on using litproc, send a message to [litproc@nist.gov](mailto:litproc@nist.gov) with the message **HELP**. To have the newsletter sent to an e-mail address other than the FROM address, contact the ITL editor.

## **MARK YOUR CALENDAR**

### **Biometric Consortium Conference 2007 (BC2007)**

Dates: September 11-13, 2007

Place: Baltimore Convention Center, Baltimore, Maryland

Sponsors: NIST, National Security Agency, U.S. Army Biometrics Task Force, Department of Homeland Security, and National Institute of Justice

BC2007 will address the important role that biometrics can play in the identification and verification of individuals in this age of heightened security and privacy by examining biometric-based solutions for homeland security as well as the utilization of biometrics in other government and commercial applications. The multi-track conference will provide a forum to address biometric research, recent technology advancements, government initiatives and commercial applications, adoption of biometric standards, and biometrics and security. The Biometrics Research Symposium will be held again this year as part of the BC2007 program. The scheduled keynote speaker is Dr. Marburger, Science Adviser to the President and Director of the Office of Science and Technology Policy.

NIST contact: Fernando Podio, 301/975-2947,

[fernando.podio@nist.gov](mailto:fernando.podio@nist.gov)

Conference website:

<http://www.nist.gov/bc2007/>.

### **Developing an Economic Strategy for Healthcare through Standards and Technologies**

Date: September 25, 2007

Place: NIST, Gaithersburg, Maryland

Sponsors: NIST, Biotechnology Council

This conference will bring together key government, industry, academic and research leaders and patient

advocates to discuss mechanisms for assessing the economic benefits and opportunities of Bio and Information Technologies and Standards in the life sciences and Healthcare Delivery and their role in bridging Healthcare system gaps. The goal is to help attendees understand the Economics of Bio and Information Technology and learn useful approaches for evaluating promising technologies. Attendees should gain an appreciation and understanding of key factors that drive the development and implementation of these technologies in the life sciences and healthcare markets and the mechanisms for evaluating the cost-benefits of these technologies.

NIST contact: B.J. Lide, 301/975-2731, [bjlyde@nist.gov](mailto:bjlyde@nist.gov)  
Conference website:  
<http://www.itl.nist.gov/Healthcare/conf/>

**Static Analysis Summit II (at SIGAda 2007)**

Date: November 8-9, 2007  
Place: Fairfax, Virginia  
Sponsor: NIST

Static analyzers are quite capable and are developing quickly. Yet, developers, auditors, and examiners could use far more capabilities. The goal of this summit is to convene researchers, developers, and

government and industrial users to define obstacles to such urgently needed capabilities and try to identify feasible approaches to overcome them, either through engineering or research.

NIST contact: Paul Black, 301/975-4794, [paul.black@nist.gov](mailto:paul.black@nist.gov)  
Conference website:  
<http://samate.nist.gov/index.php/SASII>

*Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.*